COVER SHEET

Can Organisational Failures be Prevented Before They Occur?

(A discussion about Corporate Governance and Risk Management)

Dr Paul Barnes, Queensland University of Technology, Brisbane, Australia

ABSTRACT

Given the recurrence of corporate and other organisational failures in recent years, one might wonder if both self-regulation within corporate and industrial settings and active government regulation is ineffective in an increasingly complex and changing modern world. A question that might also be asked is how (and what) organisations and governments learn from such failures? By extension it must be assumed that relevant aspects of what is learnt (or rediscovered) influences new policy or legislative change thus enhancing governance and further reducing the likelihood of future failure. With the presumption that causal and conditional evidence about such failures always awaits discovery and that humans and human systems 'learn,' the viability of anticipating future failure is self-evident.

Drawing on a number of conceptual traditions including *Normal Accident Theory* (why large complex organisational systems tend to fail), *High Reliability Organisations* (how some organisations minimise failure), and *Crisis Prone Organisations*, this paper argues that a capacity to anticipate failures and mitigate loss, is theoretically possible as a result of enhanced and directed professional practice in Corporate Governance and Risk Management. The paper also argues that while such capacities are valuable and may be sought after, the processes required to deliver organisational learning may often require adjustments outside 'the corporate comfort zone.'

INTRODUCTION

The past three decades have provided a varied kaleidoscope of organisational crises and failures to whet the appetite of observers interested in the wellbeing of national and international economies and public and private institutions generally. Incidents have ranged from large-scale corporate failures to policy-regulatory disasters with ongoing consequences to industries, global commerce and members of the public in many countries.

Notable examples within this category include failure in regulatory oversight of Mad Cow Disease in the U.K. (and more broadly elsewhere in Europe), the demise of the Barings Bank and the managerial implosions of the Enron Corp. and WorldCom Inc. to name but a few. Other examples might also be chosen from a range of industries and settings.

Could such failures be the result of bad management, the impact of unforseen circumstances or just plain bad luck? A viable consideration might also be that in the integrated post-modern world in which

we live, institutional competencies for dealing with the pre-conditions of emergent failure are not evolving as fast as the causes and co-factors of such failure. An important issue related to this point is how (and what) organisations central to such failures learn from their experience. It might be assumed that lessons learnt from direct or indirect participation in organisational loss would rapidly influence changes of policy and practice and be implemented with haste.

Questions of critical importance to both the public and private sector relate to whether the learning derived from participation in such failures can actually reduce the likelihood of future failure or at least attenuate consequent impacts. With the presumption that causal and conditional evidence about such failures always awaits discovery and that, humans and human systems do 'learn' from such events, the viability of anticipating future failure is self-evident. While such practices seem part of 'good business' it has been suggested that in the longer term, as operating circumstances change, organisations must also un-learn established practices (retain a capacity to adapt) in order to survive (Nystrom & Starbuck, 1984:53).

Establishing such an evolutionary capacity in organisations, however, requires more than the presence of strong and well-resourced internal control mechanisms derived from integrated corporate governance and risk management processes. The achievement of the dual outcome of learning and responsive control requires an openness and sensitivity to organisational vulnerability and adjustments to entrained ideas and practices that are likely to be outside prevailing corporate - managerial 'comfort zones.' While transparency is a well-known aspect of corporate governance, a regular comprehensive assessment of organisational vulnerability may not be.

This paper discusses the idea of anticipating the emergence of failure, or its pre-conditions, in organisational and regulatory settings. Initially, it outlines the nature of a range of organisational failures that have emerged from the complexity of a modern, networked world. These events are then examined in reference to empirically grounded explanatory frameworks such as *Normal Accident Theory* (why large complex organisational systems tend to fail), *High Reliability Organisation Theory* (how certain types of organisations minimise failure) and the notion of *crisis prone* organisations (cultural predispositions for failure). From this examination the paper suggests that a generic capacity to anticipate organisational failures, and thus mitigate loss, is theoretically and practically possible and presents an operational framework for structuring this capacity derived from the convergence of the practice of corporate governance and risk management.

Organisational Failure: The more things change …

Failure in human activity systems, such as businesses, governament regulatory systems, or in the provision of essential services, is not an unfamiliar event in the modern world. Some commentators suggest that such 'disturbances' are increasing in complexity and in consequence (Lagadec & Michel-Kerjan, 2004). After detailed causal analysis, incidents that on the surface seem purely technical failures often exhibit causal factors from deeper complex social and cultural contexts.

History provides an extensive retrospective of both recent and more distant organisational failures and disasters. Some incidents, such as the Tay Bridge collapse on the evening of 28 December 1879 during a severe westerly gale, have been shown to involve economic issues in addition to elements of incomplete engineering design and construction. A number of aspects of mid-Victorian industrialisation have been suggested as major contributors of the bridge collapse: a bridge building frenzy, linked to the progressive and rapid expansion of railway construction, as well as commercial competition (Pinsdorf, 1997). Key causal factors in this collapse and subsequent loss of life were determined to be a combination of unsafe and unsound design as well as substandard construction materials and on-the-job quality control (Pinsdorf, 1997). Mileham (1998), more bluntly, suggests that the bridge was built with only two things in mind - speed of construction and cost.

The Tay Bridge collapse emerged from a convergence of the socio-economic and technological advances of the time. Further, while it is an important landmark in respect to changing the way bridges were designed and constructed (Lewis & Reynolds, 2002), the collapse remains relatively uncomplicated in comparison to the breadth and depth of consequences from recent large-scale crises. Turner (1994) carried out analyses of major technical accidents over an extended period and reached a conclusion that approximately 20 to 30% of the causes of accidents sampled were technical in nature with 70 to 80% involving social, administrative or managerial factors. Social, administrative or managerial solutions were identified as highly represented in the mix of solutions defined post-incident. Given that the nature of most organisations entail humans and technology embedded together, it is logical to think of organisational failures in both the private and public sectors as elements within this broader class of socio-technical crisis.

Emergent phenomena such as climate change, public and animal health crises, the increasing hyper-complexity of embedded information-communications-technology (ICT), and the threat of terrorism can be subsumed under this category. Instances of failure from such sources are likely to generate cascading impacts through unexpected pathways and fault lines throughout the private and public sectors. Because of these cascading phenomena, institutions would be unlikely to face single incidents but rather systemic failures appearing concurrently: *a network effect.* A further point to note is that both natural and technological hazards can impact directly on human systems as well as being propagated by them. An obvious example of this propagation is the transmission of Sudden-Acute Respiratory Syndrome (SARS) internationally via business and tourist air travel.

Interestingly, commentators in the early 1990's suggested that many organisational crises may replicate in a number of common ways, yet never manifesting in exactly the same manner (Anderson, 1991). The suggestion that there are repeatable and recognisable stages in major socio-technical failure is compelling and is supported by a substantial literature grounded in the analysis of industrial and organisational settings over a number of years. Stead & Smallman (1999)[1] summarise key findings from a selection of this literature that identify five key stages in organisational failure. This are:

° *Pre-conditions* (sets of operational activity where 'signs' were buried or ignored in background noise);
° *Trigger* (an escalation factor either internal or external to an organsation or setting);
° *Crisis* (an emergent process exhibiting uncertainty and potential for loss and/disruption);
° *Recovery* (systems recovery and normalisation of functions);
° *Learning* (identification and changes to functional capacities of organisation/systems).

Table 1 presents aspects of each failure stage in respect to the collapse of the Barings Bank and the Bank of Credit & Commerce International. While differences exist between the two cases, there are a number of common aspects. The triggers for both organisational failures were diverse: one seemingly because of fraud investigations, audit reports (as well as anonymous whistle blowing) and the other, a dramatic slump in the Japanese stock market because of the Kobe earthquake. As a result of this slump, the Baring's financial exposures could not be mitigated.

Critical incidents (or multiple concurrent incidents) may be triggered at any time in large highly complex systems. Such incidents might manifest suddenly and unexpectedly or may 'cook' slowly (without recognition) until some triggering event or process precipitates them. In either case incidents can be surprising and/or unexpected. The wider literature on complex systems failure suggests that for many situations evidence is discoverable that confirms there had been 'signs' that a crisis was emerging from organisational 'noise' (Perrow, 1984; Turner & Pidgeon 1997; Boin & Lagadec, 2000; Comfort *et. al.*, 2001, Rijpma, 1997).

So if such causal factors interact within dysfunctional organisational elements repetitively, they might form a type of *vulnerability* fractal[2] manifesting as a pattern of circumstances generated by the ways in which people deal and interact with the social and technical environments in which they live and work. Support for this notion is found in the cybernetic research of Beer (1966) who suggested that while it is impossible to predict events *per se*, the pattern of interaction between *systemic* components is predictable.

1 Key works are: Turner, (1978), Turner & Pidgeon, (1997), Smith, (1990), Pearson & Mitroff, (1993) and Pearson & Clair (1998).
2 The term fractal as coined by Mandelbrot originally referred to shapes that are "self-similar" that is - looked the same at different magnifications. My meaning here is more metaphorical but is intended to convey that certain causal and explanatory factors, identified retrospectively, seem to have common bases and recur to a consistent degree

Table 1: Stages of Organisational Failure: Barings Bank and The Bank of Credit & Commerce International

(Derived from Stead and Smallman, 1999)

<table>
<tr><th></th><th>Barings Bank</th><th>The Bank of Credit & Commerce International</th></tr>
<tr><td rowspan="2">Pre-conditions</td><td>° Ill-defined and complicated Corporate Structure (Confused reporting lines & accountabilities)
° Few staff experienced at futures trading
° Unregulated & growing market
° Senior management seemed unaware of the potential for loss from financial activities</td><td>° Complicated organsiational structure
° Unprecedented growth in global banking
° Fraudulent activities of senior staff</td></tr>
<tr><td colspan="2">Common Issues:
° Communication gaps among regulators
° Un-prepared for crisis situation
° Failure by auditors to detect unusual transactions
° Inadequate monitoring by senior authority
° External parties aware of some degree of irregularity</td></tr>
<tr><td>Trigger</td><td>° The ‘plunge’ of the Japanese stock market following the Kobe earthquake</td><td>° A report by Price Waterhouse Coopers
° An anonymous tip-off
° Action by the New York Attorney General</td></tr>
<tr><td rowspan="2">Crisis</td><td>° Focused on futures trading and individual fraud
° Losses of approximately USD$15 billion</td><td>° Bogus loans & external funds - predominately multi-individual fraud
° Losses in excess of USD$927 million</td></tr>
<tr><td colspan="2">Common Issues:
° Severe impacts on the financial industry and the economy
° Extensive media coverage</td></tr>
<tr><td>Recovery</td><td>° Barings purchased by ING</td><td>° BCCI ceased trading</td></tr>
<tr><td>Learning</td><td colspan="2">Common Issues:
° Management had little opportunity to learn due to BCCI’s closure and Barings being absorbed by another organisation.</td></tr>
</table>

Ringland *et.al.* (1999) noted a number of cultural factors prevalent in organizations, indicating a generic inability to anticipate future conditions. These are 'not paying attention;' 'losing messages amongst internal noise;' 'overconfidence in expertise;' and 'assumptions of adequacy.' The latter two of this list might have been pertinent in the Barings Bank collapse especially in terms of the activities of key personnel described as 'not sufficiently experienced to realise the potential dangers' of their actions (Stead & Smallman, 1999). The reality of complex networked systems, as evidenced by the growth of the internet and the world-wide-web, has enabled the ubiquity of *e*-commerce and other evolving forms of virtual communication as mainstays of the modern world.

The efficacy of 'networked" systems as both a descriptive and analytical tool within international business settings, especially in logistics and supply-chain management, has great credence. This is particularly pertinent given that there are an estimated 250 million maritime cargo movements each year (circa 2003) and that up to 90% of world cargo movement occurring in shipping containers (OECD, 2003). The size and complexity of the logistics systems that underpin these numbers staggers imagination.

Mahon & Cochran (1991) have suggested that the use of aspects of complexity theory as a conceptual and analytical tool within commerce, organisational design and functioning would become a paramount factor in effective corporate and operational management in the public and private sectors globally. More recently, Robertson (2004) has supported this contention. While the application of these concepts seem both reasonable and logical, implementing processes to accommodate such an extension is likely to generate much activity for consultants - both internal and external to firms.

The return-on-investment from such activities however may not be easily delivered. While complexity theory is rich in examples within ecological and natural systems, it would be critical to have empirical basis for analytical frames grounded in organisational functioning, and in this case dys-functioning. Without these bases to guide understanding of how organisations and institutions operate as they fail, or edge towards failure, remedial management options would remain limited.

Crisis management theorists have emphasised the need for strategists to extend their traditional conceptual frames and stakeholder maps from models of the *world as a simple machine* to the *world as a complex system* (Mitroff & Kilmann, 1984). The drawing of analogies between biological systems and socio-technical systems, while once not a part of mainstream management science, has been validated or at least accepted by many thought leaders and trans-disciplinary researchers (Holling, 2001). In this sense, circumstances under which expected organisational functioning 'transitions' from normality to crisis, may be an analogue of moving from regularity (familiar - expected functioning) to the edge of chaos (unmanageable complexity).

Ways of Seeing: analytical frameworks

Given the complex factors in organisational failures and the tendency for such events to 'fractalise,' access to workable conceptual and explanatory frameworks for policy development and risk management processes are critical. An operational understanding of the emergence of crises into 'normal' everyday life (and organisations) requires individuals and groups to 'make sense' what is occurring to them, and around them.

Recognition of the generic stages of a crisis is important but such external categorisation does not necessarily allow a conceptual understanding of the causes of a crisis. A number of pivotal conceptual schemas, specifically related to organisational failure and crisis mitigation and derived from empirical evidence from both post-failure analysis and functional organisations, are available in the literature. Three framework-themes are examined to establish a basis for developing a deeper understanding of organisational failure: *Normal Accident Theory*; *High Reliability Organisations* and *Crisis Prone Organisations*.

Normal Accident Theory

Normal Accident Theory (NAT) emerged from analysis of a range of industrial disasters and accidents spanning a period of at least the last 40 years. Such incidents include the chemical release at the Union Carbide plant at Bhopal (India), the 1979 accident at the Three Mile Island nuclear power plant and many others. Perrow (1984) introduced the idea that in some technological systems, accidents are inevitable or 'normal.' He defined two related dimensions - interactive complexity and loose/tight coupling - that defined organisational susceptibility to accidents (Marais *et. al.*, 2004).

The notion of interactive complexity includes two factors: *Linear* and *complex* interactions. Linear interactions are elements in expected or planned operational sequences. The attributes of linear systems generally behave in planned ways with single functions. Interactive complexities, however, derive from unfamiliar, unplanned or unique operational sequences that might not be visible or comprehensible to users of the system (Perrow, 1984). Table 2 displays generic differences between complex and linear systems.

The critical aspect this dyad is comprehensibility: with linear interaction deemed more easily understood than complex interactive phenomena. This does not mean linear equates to 'simple' as many very complicated systems do not exhibit strong interactive complexity. Perrow (1984) suggested that linear systems exhibited fewer feedback loops than found within non-linear systems. The potential for interactive complexity emerges from the likelihood of unfamiliar and/or unexpected sequences of events linked to feedback processes.

Table 2: Characteristics of Complex and Linear Systems (Perrow, 1984)

Complex Systems	Linear Systems
° Components closely packed ° Non-varying sequences ° Interconnected sub-systems ° Many feedback loops ° Multiple / interacting controls ° Indirect information	° Components spatially segregated ° Sequence order can be changed ° Segregated sub-systems ° Few feedback loops ° Segregated controls ° Direct Information

The second explanatory dimension; 'coupling' is defined as the degree of slack or redundancy between system components. Organizations with loose coupling for example may have flexible performance standards with less time-dependencies and a capacity for 'last-minute' resource and process substitution. Tightly coupled systems on the contrary possess elements whose functions are highly interdependent with other sub-systems, and linked relationally in space and/or time. Therefore, a change in one part can rapidly affect the status of other parts. Table 3 details tendencies of both forms of coupling.

Table 3: Characteristics of Tight and Loose Coupling (Perrow, 1984)

Tight Coupling	Loose Coupling
° Processing delays not possible ° Non-varying sequences ° Single methods used ° Little 'slack' possible in supplies, personnel or equipment ° Buffers & redundancies are deliberate and designed in	° Processing delays are possible ° Sequence order can be changed ° Multiple methods are available ° Slack in resources possible ° Buffers and redundancies available are applied as needed

Perturbations in tightly coupled systems can show an effect quickly, often with serious and disastrous consequences. NAT defines loosely coupled or decoupled systems as having fewer or less 'critical' links between parts and therefore able to absorb failures or unplanned behaviour without significant destabilisation.

According to theory, systems with interactive complexity and tight coupling have increased potential to experience accidents that cannot be foreseen or prevented. Perrow (1984) refers to these as 'system' accidents. When the system is interactively complex, inter-dependent failure events can interact

in ways that cannot be predicted by the designers and operators of the system. If the system is also tightly coupled, the cascading of effects can quickly spiral out of control before operators are able to understand the situation and perform appropriate corrective actions. The loss of control was a strong possibility during the Three Mile Island nuclear reactor Incident. In such systems, apparently trivial incident can cascade in unpredictable way and with possibly severe consequences (Marais *et. al.*, 2004).

Systems accidents result form a gestalt of the processes not the component parts themselves. The practical importance of NAT is that it allows observers to comprehend the interaction and flow of events in difficult and ambiguous situations as organisations deal with unexpected events. The explanatory power of the 'linear and interactively complex systems' terminology, central to NAT, was a key reason it was included in the language used by the investigating Commission to describe the Columbia shuttle disaster (Weick, 2004). A further element of value is that NAT focuses on structural factors and combinations of problems instead of on isolated errors of individual human operators or design flaws in individual components. This focus allows scrutiny of the structural underpinnings of organisational systems and the often intricate and unexpected causes of system failure (Jermier, 2004).

High Reliability Organisations

High Reliability Organisations (HRO's), as the words suggest, are closely linked to safety, regularity and accuracy. Roberts (1990) suggests that if the answer to the question 'how many times could this organization have failed resulting in catastrophic consequences but did not' is in the order of tens of thousands of times, then that organisation exhibits 'high 'reliability.

To achieve this HRO's operate in a context of near full knowledge of the physical and technical aspects of the operational activities they carry out. People in these organisations know almost everything technical about what they are doing and aim at having prepared for nearly every conceivable contingency. Aircraft carriers within the US Navy have been a major empirical source of data about HRO theory development (Roberts, 1990a; Roberts1990b; Roberts, Rouseau & La Porte, 1994).

This drive for predictability in HRO's and candidate HRO's has resulted in the adoption of relatively stable technical processes that are well understood by participants. The 'deep' safety - reliability aspects of an existing work culture is imbued into new workers from their first day. Beyond this socialisation process, a higher goal of functional systems is that interactive complexity is designed-out of processes to the greatest possible extent. A further factor is that task specifications and functional designs are unchanging, or very slowly changing, and that maximal learning is sought after accidents and incidents (Marais *et. al.*, 2004).

The tendency to seek and require complete knowledge of a system or process by HRO's contrasts against the 'interactive complexity,' described by NAT where the interactions between components cannot be thoroughly planned, understood, predicted, or guarded against. Ideally for HRO's, it would be relatively easy to lower risk through standard system safety and industrial safety approaches. Unfortunately most complex systems, particularly high technology and social systems, do not fall into this category (Marais et. al., 2004).

Crisis Prone Organisations

Henry Kissinger is reputed to have once said that .. "I don't have time for a crisis next week my schedule is already full." While the humour of such a statement is obvious evidence derived from the crisis management literature would suggest that many organizations possess a range of vulnerabilities that, in effect, predispose them to failure often without self-awareness or recognition of existing susceptibility.

Analyses of iconic organisational failures and their aftermath have shown that in addition to certain causal triggers of crises being unexpected and predisposing factors overlooked (as evidenced in Table 1), the capacity to respond quickly and appropriately once emergent signs appeared also seemed restricted. Specific organisational cultural patterns or 'operating rules' have been retrospectively linked to the genesis and amplification of well-known organisational crises. It has been strongly argued that the presence of such patterns in an operational repertoire increase vulnerability and the likelihood of accidents and crises (Perrow, 1984). Of the many that have been examined three pertinent examples are noted here. These are:

- *Rigidity in thinking:* Restricted expectation about contingencies and their consequences, inflexibility in considering alternative options & choices for mitigation;
- *Information Distortion:* Attenuation and filtering of information to key decision makers;
- *Lack of Decision Readiness:* Key decision makers not practiced in emergency decision making.

(Smart & Vertinsky, 1977)

The explosion of the Challenger space shuttle exemplifies bureaucratic attenuation of information flow and rigid viewpoints. A number of investigations after the incident called attention to the fact that people within engineering areas of the launch group repeatedly expressed concern, sometimes quite forcibly, about the potential dangers of launching the Challenger under low-temperature conditions. It is interesting to note that persons at the top of the organisation reported never having heard anything about such concerns during the same investigations (Freudenburg, 1992).

Information filtering can lead to a reduced organisational capacity to make operationally difficult decisions. Further, over time, attenuation of information especially if it relates to the functioning core of sub-systems can lead to organisational blindness. Patterns such as these that support the 'incubation' of

failures and the inability to note the presence of 'warning signs' are symptoms of crisis prone organisations (Turner & Pidgeon 1997; Pearson & Mitroff, 1993; Mitroff & Alpaslan, 2003). Crises and their consequences might also be seen as caused not just from the failure to notice signs, but also from a failure of organisational systems to respond to them.

The Exxon Valdez oil disaster exhibits aspects of all three of these cultural phenomena. While shipping in and out of the Alyeska pipeline terminal in Valdez (Alaska) had not been totally free of incidents, the generally safe pattern of experience up to mid-night on March 23rd 1989 is unlikely to have raised concerns about catastrophic failure for most observers. Over a period of more than a decade up to the incident, approximately 8,000 tankers had gone in and out of the port without a single catastrophic failure. Five minutes later, however, a sophisticated oil tanker that was literally miles away from its original plotted course had an incredibly stupid encounter with a submerged obstacle (Freudenburg, 1992).

Past success (or lack of failure) can inculcate restrictive beliefs about what might happen in the future and generate assumptions about reduced vulnerabilities for individual actors and organisations. A further set of unrealistic expectations about contingencies and capacity to respond were embodied in extant emergency plans for Prince William Sound and the surrounding terminal infrastructure. A number of contingency plans were in effect at the time of the spill (Clarke, 1989). These included:

- The National Oil and Hazardous Substances Pollution Contingency Plan,
- The Coast Guard's Captain of the Port Prince William Sound Pollution Action Plan,
- The Alaska Regional Oil and Hazardous Substances Pollution Contingency Plan
- The State of Alaska's Oil and Hazardous Substances Pollution Contingency Plan,
- The Alyeska Pipeline Service Company's Oil Spill Contingency Plan for Prince William Sound.

General expectations embodied in these plans assumed that rescue and response equipment would be at the ready and that this material would be deployed in a carefully coordinated manner, with an efficient and effective division of labour among organisations being instituted almost immediately. A further expectation was that clear, open and honest communication channels would be established readily among previously competitive or even adversarial organizations and that each responding organisation would take precisely the right step at precisely the right time to fit the need of other organizations (Freudenburg, 1992).

The reality was that confusion seems to have been far more commonplace than communication. Rather than coordinating their activities the various organizations with a stake in the spill and the clean-up often seemed to have more interest in blaming one another than in working together (Freudenburg, 1992).

Lack of decision readiness and unrealistic assumptions about roles and actions to be carried out by relevant actors can lead to a state of operational gridlock. The contingency planning in place at Prince William Sound has been described as reflecting organizational perceptions regarding possible catastrophes and their nature, and belief that the likelihood of oil spills had been thoroughly considered. Such plans were intended to convey that the organisations were in control of a potentially uncontrollable situation (Clarke,1993). When informed of the incident with the Exxon Valdez U.S. Coast Guard Vice-Admiral Clyde E. Robins is reported to have said this was impossible as we have the perfect *preventive and contingency* system (italics added) (Egan, 1989).[3]

The Surprise Factor: Learning, Un-learning or just forgetting?

Surprise has always had an egalitarian affect in society. To be pleasantly surprised is more preferable than the alternative. The alternative state unfortunately has, as shown above, been present more often than not in many organisational crises. The absence of surprise within organisational operations could be an important sign that regulatory control systems operate as expected and are in place to deal with functional requirements of normal operations.

There are many instances where failures are so significant that permanent changes occur in complete bodies of knowledge and professional practice. The Tay Bridge disaster, as mentioned earlier, instigated important changes in bridge design, construction and inspection (Lewis & Reynolds, 2002). Equally, failure can also instigate wholesale changes in institutions both public and private. Examples from the corporate world such as Enron and WorldCom have influenced the introduction significant new legislative regulations for financial reporting and governance generally. The Sarbannes-Oxley Act in the U.S. and the Corporate law Economic Reform Program (CLERP 9) in Australia, both introduced in 2002, are examples of the regulatory reactions (learning) to recent corporate failure.

Equally, the public sector has not escaped post-failure change. In the U.K the changes made to the Ministry of Agriculture, Food and Fibre (MAFF) in the wake of the Bovine Spongiform Encephalitis (BSE) crisis are a point in fact. Almost instantly within the normally slow bureaucratic time space, MAFF became the Department of Environment, Food and Rural Affairs (DEFRA). This re-badging, in marketing terms, might be construed as an enforced 'un-learning' to adapt to external pressures from concern about the management of the BSE crisis, not only by the public but also from a political perspective.

An important factor in most aspects of crisis management is, of course, decision making. Usually this will be carried out under considerable stress (due to time sensitivity and the importance of 'getting-it-

[3] Reported by Clarke (1993).

right') and uncertainty (including confusion and ignorance). In generally well-known socio-technological settings (as in HRO's) the uncertainty may be less a factor for decision makers

The role of government in preventing such failures is critical in that varieties of the 'modern state' as functional providers of public administration and governance derive validity from the promise that it is an effective (and preferred) form for the provision of safety (and certainty) in society. This role is made more important because in representative democracies, it is a reality that many decisions with potential to affect our lives are made by others. Such power differentials can manifest as intractable concerns among members of the public who find themselves distant from the decision-making processes (Luhmann, 1990).

Of equal importance are questions about the role of the private sector in generating and promoting new technologies and sustaining established ones, especially within the mélange of supply, demand and consumption. In addition to a diverse literature recognising issues of public trust and perceptions of the credibility of institutions there has been a recent expansion of policy development and enhanced professional dialogue in Europe and elsewhere focusing on the implementation of governance frameworks that are inclusive of the needs of a range of stakeholders.[4]

Beyond questions of public confidence in regulatory authority a further issue for government is the regulation of science and the support of economic activity. It is common for modern government(s) to actively support and promote innovation for the betterment of society. An ongoing task for government as it endeavors to support such development is how to bring the management of scientific innovation and the promotion of technology into the public arena and thus into a mainstream democratic discourse (Giddens, 2001).

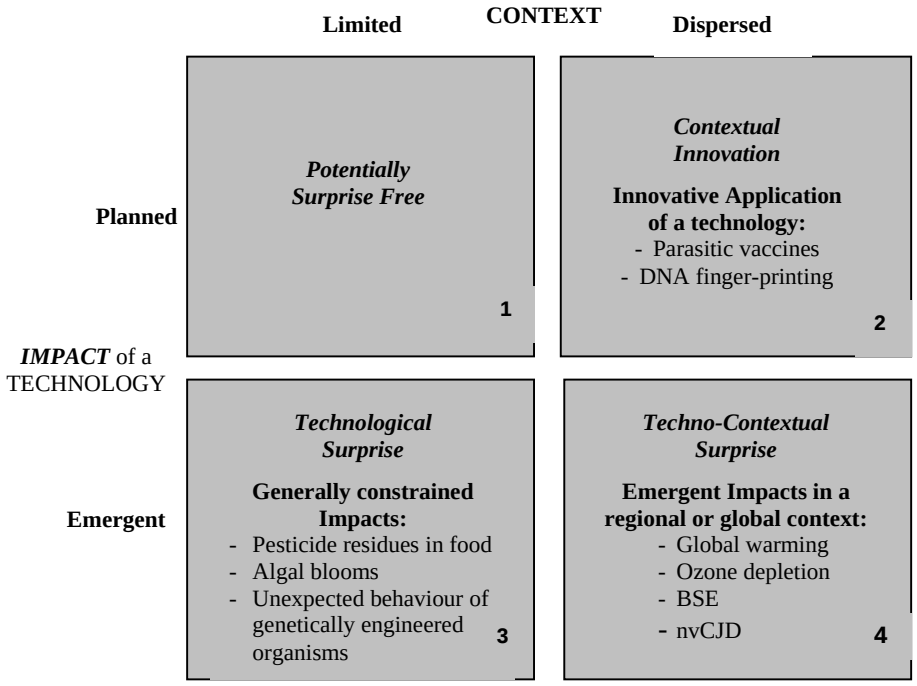
An extension of the notion that government 'makes safe' is the expectation that it also licenses and regulates the use of technology, and by doing so, provides a degree of certainty about predictability and safety of it's use. It is here that risk management and technological foresight are critical: especially as it applies to regulatory organizations. This especially holds in relation to reducing the likelihood that incidents or issues involving the impact of technology or regulatory safety develop into crises.

Paradigmatic science, in a Kuhnian sense, and its cousin standardized technology, is expected to be relatively surprise free. Unexpected impacts from the application of technology can and do occur often with higher order consequences that extend over dispersed geography often with inter-generational impacts. Figure 1 explores this issue in greater detail.

[4] The TRUSTNET Framework (A New Perspective on Risk Governance) circa 1999, and more recently "Trustnet-in-Action."

A suitable goal of effective public and private oversite of technology might be to minimise generation of outcomes as shown in segment *3* and *4*, while promoting policies that seek to support achieving the relatively benign state in segments *1* and *2*. The emergence of segment *3* or *4* impacts may be difficult to predict because of unnoticed trends, an unanticipated synergism between components of complex systems[5] or by a discontinuity (an abrupt shift in a previously stable system or context).[6] From an NAT perspective emergent impacts such as those in segment *4* cause surprises because they manifest from a higher order of interactive complexity.

Figure 1: Limited and Dispersed Impact of a Technology
(Barnes & Hulsman, 1995)



Marais *et. al*. (2004) suggests that organisations such as NASA or any that develop and/or use advanced technology, across a range of disciplines, do not always have detailed experience from which to form the basis of familiarity and "learning." Experience with old technologies might not be applicable to newer ones. For example, digital systems such as fly-by-wire avionics or transnational information and communication technology systems may in fact affect the frequency, nature and understandability of accidents.

[5] Examples of Segment 4 impacts: The discovery of BSE in cattle related to the use of meat and bone meal products in feed and the admission that zoonotic transmission was likely to be a major causal factor (if not the cause) of a significant increase in cases of new variant Creutzfeldt-Jakob disease.
[6] Over use of a natural resource either by grazing or over fishing could affect the reproductive success of some flora or fauna to the point where the sustainability of that resource is significantly disturbed and it is forced into a rapid and irreversible decline.

Marais *et. al*. (2004) further suggest that advanced technical systems might change the type of errors made by operators and that experience with older, electro-mechanical systems have little evolutionary link to new system designs and technology. It is from this type of context that *normal accidents* and techno-contextual surprise emerge.

If such incomprehensibility factors are combined with an organisational culture that is crisis prone with heritable characteristics such as, rigidity of core beliefs, values and assumptions of competency, ineffective communication and information sharing capacities, and a misplaced belief in of its own expertise, the organisation may be incapable of learning and in generating flexible responses (Smith, 1999). Referring again to recent snapshots of organisational culture in NASA, Mason (2004) suggests that the causal context of a failure may reach a considerable distance back in organisational history. The agency's long string of previous successes, however, may have led its managers to believe that they could do no wrong. This attitude of omnipotence is very dangerous when dealing with complex, unruly, ultimately unpredictable technology (Mason, 2004).

An important issue in the modern world of e-commerce and interoperability is the potential for unexpected convergence of crisis elements to impact on human systems and generate effect propagation via the inter-connectedness of these same systems. Lagadec & Michel-Kerjan (2004) refer to such a tendency to ubiquitousness as a 'Network' factor. By escalating the notion of a *normal* accident to consider global interdependencies and globally tight couplings we might have seen in recent events, real-time discontinuities that create situations where an understanding of the settings and contexts of crises eases beyond the grasp of competent authorities to make sense of the trajectory of events. Crises such as these are often described as 'outside of the box,' 'too fast,' 'too strange' and 'too costly' (Lagadec, 2004). It is in such circumstances that preventing critical network events and the surprise they bring is critical.

Decision making, and even providing reasoned advice, is extremely difficult in circumstances where organisations are surprised by internal or externally sourced failure. Given the convergence of information, actors and factors within crisis situations a critical question is how officials make sense of the complexity surrounding them and how such developed awareness influences decision making (Weick, 1988).

Learning is also a form sense making which, in retrospect, illuminates how decisions were and were not made. The reaction of Winston Churchill after the fall of Singapore in WWII is an interesting consideration. Allison (1993) notes that he asked four questions in his role as leader: "why didn't I Know," "why wasn't I told," "why didn't I ask," "why didn't I tell what I knew?"

By logic, no one person could ask these questions and by extension, it would take organisational knowledge to answer them. It may be that organisational learning starts with ensuring the presence of internal capacities to ask such questions in advance of being surprised and then determining if organisational policies and functional systems support the effective and timely delivery of the answers.

***Anticipation*: A Convergence of Corporate Governance and Risk Management**

A key factor in the literature and professional practice of crisis and disaster prevention is early warning and effective communication (Wisenblit, 1989). As suggested earlier, faulty or untimely communication is implicated in many well-known organisational crises. The failure to notice signs in the pre-condition phase of a failure process may not just be the result of inattention but a compound issue of both deficiencies in the communication mechanisms and differences in functional worldviews between layers of an organisational hierarchy.

Weir (2004)[7] states that timely communication can be filtered out because 'upper layers' of management may find the content inappropriate or unacceptable. Analysis of events leading to the loss of the space shuttle Columbia indicate that NASA officials initially rejected the foam strike as the proximate cause of the accident and as a matter of faith held steadfastly to that belief, even in the face of accumulating evidence and strong interventions of in-house engineers. It is reported that such rigidity in belief was held by some members of the managing hierarchy that requests to gather more evidence via satellite or telescopic imagery were denied (Mason, 2004).

Such unwillingness to listen to advice, especially when signals of emergent failure were present is at odds with historical practice in an earlier incarnation of NASA under the directorship of Werner von Braun. von Braun used a communications practice referred to as 'Monday Notes' to elicit direct and timely feedback to and from mid-level project managers about problems or issues that arose in the previous week. von Braun personally made notes and put suggestions on the single page reports. All 'notes' were copied and returned to the full management cohort. As a result, upward and horizontal communication was enhanced (Tompkins, 1993). Such orchestrated transparency would be unique even today.

Lagadec and Michel-Kerjan, (2004) suggest that high-level executives may feel deeply threatened by the thought of promoting unpopular advice or views on emerging threats. In such instances it could be common to treat such threats as 'unrealistic', 'too rare', 'beyond our responsibility,' quoting a lack of historical data and difficulty in measuring the emerging threats in metrics with which they and their board were familiar.

[7] Referencing: Beer (1966) & Revans (1982).

Corporate governance is grounded in the effective use of information management and control mechanisms (Turnbull, 2002:261). An adequate capacity for corporate governance therefore would require the existence of a variety of channels of information to senior decision makers. However most people with experience of working within either the public or private sector would appreciate that because the generation of information is a human-centred process, like the application power, communication channels are invariably clogged with bias, distortion and 'noise. Advice about overcoming this arteriosclerosis of information flow by creating multiple sources of information (formal and informal) and mechanisms for propagating it, spans a range of literature over a number of years (Shannon, 1949; Beer, 1995).

The importance of systems complexity in explaining organisational failure has been noted extensively above. Effective corporate governance also requires capacities for coping with this phenomenon and structuring suitable internal control mechanisms. With suitable reporting mechanisms in place, enhanced variety in strategic information creation can be developed to generate increased capacity to attenuate corporate risk.

The recognition of managerial structures, in circumstances of complexity, is supported conceptually by the 'Law of Requisite Variety' (Ashby, 1986). Clearly stated, this aphorism suggests that the variety of a regulator (or control system) must equal that of the variety of the situation being regulated. Thus as organisations increase in complexity and opaqueness, so too must the sophistication and variety of acquisition of corporate information and regulatory control.

While sophistication of the information in such circumstances is a given, it must be timely, be couched in forms that aid decision making and not impede it. Additionally, there is no causal link between extra information and better decisions. In fact too much information or an influx of new data can detract from balanced decision making. Full awareness of these issues is central to creating useable knowledge as a decision support aid in uncertain contexts (Sarewitz & Pielke Jr., 2001).

How could a convergent Corporate Governance - Risk Management framework that caters for these information issues be structured? Figure 2 displays a possible operational structure designed to both minimise the emergence of the signs and symptoms of organsiational failure and identify them should they appear. It has been in use within a large public sector organisation in Australia for some time. The agency in question has the same general regulatory responsibilities as the UK Department of Environment, Forestry & Rural Affairs but covers a State with a jurisdiction many times that of the United Kingdom.

The framework comprises a standard internal control capacity embodied in an Internal Audit committee with an expanded governance capacity in the form of separate Legislative and Finance committees. It also includes a separate Corporate Risk Management Committee (CRMC). All four

committees report in parallel to the Departmental Board of Governance. The Legislative Committee provides advice on legislative reform related to departmentally regulated matters and external legislation. The Finance Committee, as might be expected, ensures accurate and detailed reporting of financial statements to the Board.

The CRMC provides a department-wide forum for the promotion of risk management principles and techniques, and its members contribute to the management, direction and planning of risk management projects and tasks within the department. It comprises representatives from the other three committees and includes risk management specialists. The committee also acts as a filter for threat and risk issues cutting across the legislative or professional responsibilities of the other committees. For example, a legislative development external to the organisation that had obvious impacts on policy implementation could have impacts on projected budgets. A more complete picture of these issues is then aggregated by the CRMC into a combined assessment of departmental exposure.

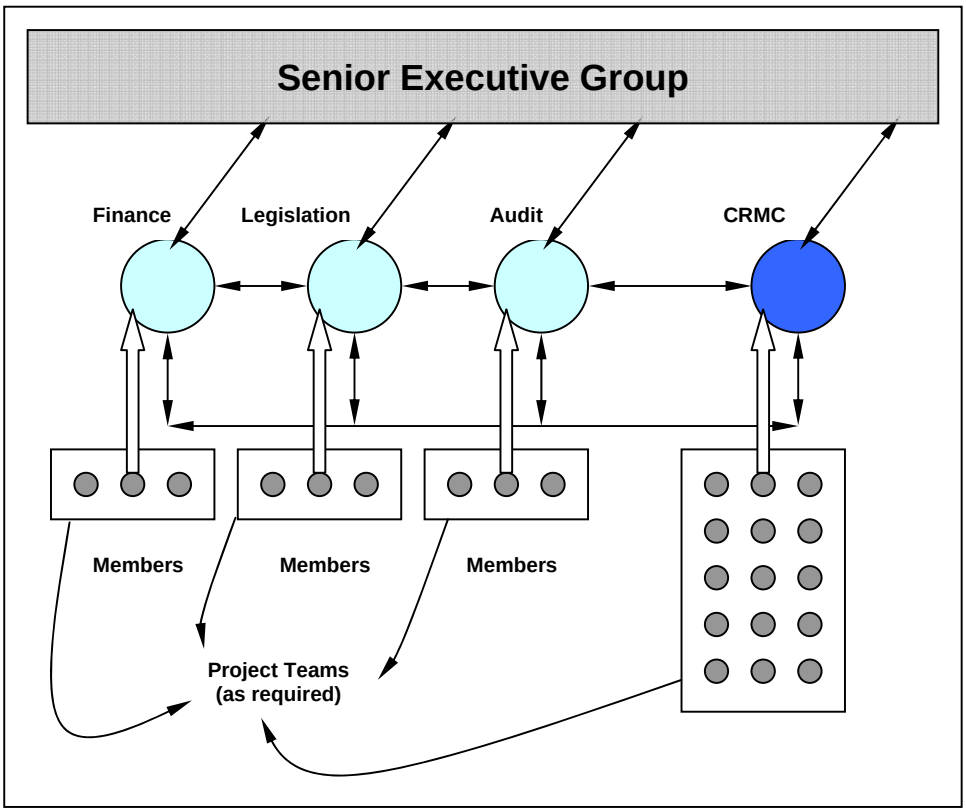
An eclectic view on the combined exposures would allow comprehensive and robust organisational mitigation strategies to be chosen and implemented. A key function related to this strategic view is the preparation of a Corporate Threat Register.

The Corporate Threat Register (CTR) is used a decision-making aid by the Board of Governance to prioritise risk management activities, decision making and enhance governance generally.

The purpose of the CTR is to provide the means to:

- Support a process to identify key issues that may emerge as a crisis and determine prevention and/or mitigation strategies;
- Accommodate multiple technical and professional perspective's on risk and loss and differing regulatory needs across a diverse public sector portfolio;
- Produce consistent and rigorous risk analyses to support decision-making functions of the Board of Governance the face of varying degrees of certainty (Barnes, 2001).

Figure 2: **A Corporate Risk Management Framework**



Design specifications for the register include the functionality for identifying and documenting:

- Strategic *threats* that could affect the standing of the Department and/or reduce the likelihood of achieving strategic goals and objectives;
- Information about identified threats and recommended mitigation strategies for decision makers;
- Threat-related information in a form that supported effective decision making and was derived from a robust and standardised risk analysis methodology;
- Mitigation strategies and accompanied implementation plans across the organisation;
- Individuals or groups responsible for implementing mitigation strategies (Barnes, 2001).

A higher order purpose of the Corporate Risk Management Framework shown in Figure 2 is to overcome any propensity of the department to become crisis prone and succumb to the many interactive complexity and coupling factors present in such a large and diverse public organisation. By engaging in a structured analytical process the benefits of strategic foresight, issue and scenario analysis and the engagement of expertise at all levels of the organisation, a capacity to recognise unexpected and usual

changes in organisational functioning is part of the register's design goal. The inclusion of these capabilities is well supported in the relevant literature (Kash & Darling, 1998).

Particular attention during the implementation of the framework focussed on ensuring information flow(s) to the governance committees and from them to senior executives. The combination of specialists (in the legally mandated committees) and generalists guided by specialist risk professionals in the CRMC is designed to address the 'Law of Requisite Variety' described above. By designing the team and its functional processes to match organisational complexity, it is hoped that unexpected surprises could be minimised and that information and advice on corporate governance matters would flow smoothly and in a timely manner to the highest levels of the organisation.

Clarke (1993) raises important points about how data becomes information in large and complex organizations especially when crisis approaches:

> *The process here concerns how data are turned into information. Modernity, and its increasingly complex socio-technical systems, are inundated with raw data, about o-rings, nuclear designs, occupational hazards, and so forth. How those data are organized and made sense of determine whether they become relevant information or are dismissed as background noise. It would be surprising if degree of professional specialization were irrelevant to those processes.*

Conclusion

How might recognition and use of such combinations of Corporate Governance and Risk Management capacities be promoted domestically and internationally? Mendonça, (2004) suggests that in certain circumstances 'weak signals' might be discernable that are not necessarily inimical to an organisation but might be the harbingers of novelty and innovation. The organisational capacities to discern opportunity and threat are similar and access to an organisational repertoire that allows both outcomes would be a much sought after benefit. Such capacities, however, require committed and sustained investment in human resources and organisational flexibility. It is only through such commitment that effective corporate governance outcomes may be achieved.

A commitment to a sustained ability to examine organisational vulnerability can be unfashionable because corporate governance and crisis reform is essentially cyclical. Corporate governance reform and increased regulation is generally more active during periods of recession, corporate collapse and re-examination of the viability of regulatory systems (Clarke, 2004). Support and active interest in the conformance aspects of governance diminishes during periods of expansion as companies and shareholders become again more concerned with the generation of wealth.

This paper has argued that failures are a normal and expected aspect of large interactively complex organisations. It has also suggested that when organizations learn from errors and crises there is a tendency towards forgetful-ness, ambiguity and uncertainty over time. Aspects of these conditions have been teased-out by brief examinations of the three empirically grounded conceptual themes from crisis and risk management literature.

Crisis management is effectively a shorthand for management practices subsumed into institutional and organisational responses to non-routine events. Rhinard, Ekengren, & Boin (2004) suggest that specific challenges can be categorised under four headings: *Prevention* - recognition systems for emerging crises; *Preparation* - planning for the unknown; *Response* - making effective decisions and having them implemented; and, *Recovery* - restoring normality and learning. However, both *preventing* and *preparing* for crisis-situations presumes a deep and effective understanding of the way in which 'unknown' factors and conditions can manifest. Understanding further presumes a means to do this that allows sense to be made of confusing circumstances. Equally important is the capacity to effectively generate an organisational response in crisis situations.

Complacency concerning corporate governance and risk management during uneventful times compounds the impacts of crises when they occur. Such factors are universal in market systems and in socio-technical settings but because of differences between international systems of governance the unwinding of this saga have occurred at varying times, for different reasons, and with different primary and secondary consequences (Clarke, 2004).

Finally, Mason (2004) details excerpts from findings of the Commission of Inquiry into the loss of the space shuttle Challenger that state: "Thiokol Management reversed its position and recommended the launch of [*Challenger*], … contrary to the views of its engineers in order to accommodate a major customer." The Commission report further states that "NASA appeared to be requiring a contractor to prove that it was not safe to launch, rather than proving it was safe." Arguably this disaster was destined to occur because the 'institution' behind the space shuttle had lost its capacity for high reliability, failed to sense the vulnerable state decision-making processes had created, and had become crisis prone. In this sense it was an orgnaisational failure that probably could not have been prevented before it occurred.

LIMITATIONS OF THE PAPER AND FUTURE DIRECTONS

This paper bases its arguments and comments on established conceptual frameworks grounded in empirical research. It is by design theoretical and analytical but does identify clear directions for further investigation. While the Framework shown in Figure 2 is currently functional in a large and complex

public sector organisation there is a need to assess more formally the viability of its basic design and conceptual foundations. This includes how well its conceptual basis and design parameters match different operating environments and settings in public and private organisations internationally.

Examination of the application of 'the law of requisite variety' in the preparation of corporate threat assessment teams as well as the usefulness of separating formal internal control processes from anticipatory corporate risk functions would also be timely. This latter question is important for enhancing corporate governance and minimising organisational vulnerability and failure in domestic and international firms both publicly listed and held privately.

REFERENCES

Allinson, R.E. (1993). Global Disasters: Inquiries into Management Ethics. Prentice-Hall, New York.

Anderson, A. (1991). Making a Success out of a Museum of Failure. New scientist, 130, p. 54

Ashby, W.R. (1968). An Introduction to Cybernetics, University Paperback, London.

Barnes, P. and Hulsman, K. (1995). Ecological Risk Analysis of Transgenic Plants. Proceedings of the 1995 ANZAAS

Barnes, P.H. (2001). Organisational Vulnerability in the Public Sector: A Case Study in the Design of Corporate Threat Registers. In the 25th National Conference of Australian Risk & Insurance Managers Association, Canberra, 18-21 November.

Beer, S. (1966). Decision and Control, Wiley, London.

Boin, A. and Lagadec, P. (2000). Preparing for the Future: Critical Challenges in Crisis Management. the Journal of Contingencies and Crisis Management, 8(4): pp. 185-191.

Clarke, L. (1989). Organizational Foresight and the Exxon Oil Spill. In an Unpublished paper, Department of Sociology, Rutgers University.

Clarke, L. (1993). The Disqualification Heuristic: When do organizations misperceive risk? Research in Social Problems and Public Policy, Vol. 5, pp. 289-312

Comfort, L. *et. al.* (2001). Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments. Journal of Contingencies and Crisis Management, 9(3): pp. 144-157.

Egan, T. (1989). Elements of tanker disaster: drinking, fatigue, complacency. the New York Times, May 22.

Freudenburg, W.R. (1992). Nothing Recedes Like Success? - Risk Analysis and the Organizational Amplification of Risks, Vol. 3.1 of the Indexed Risk Articles of the Franklin Pierce Law Centre (URL: HTTP://WWW.FPLC.EDU/risk/rapa.HTM).

Giddens, A. (2001). The Second Globalization Debate: A Talk With Anthony Giddens. The Edge Interview: www.edge.org/3rd_culture/giddens/giddens_index.html

Holling, C.S. (2001). Understanding the Complexity of Economic, Ecological, and Social Systems. Ecosystems, 4, pp. 390-405.

Jermier, J.M. (2004). Complex Systems Threaten to Bring Us Down … Organization & Environment, 17(1), pp. 5-8.

Kash, T.J. and Darling, J.R. (1998). Crisis Management: prevention, diagnosis and intervention. Leadership & Organisation Development Journal, 19(4), pp. 179-186.

Lagadec, P. (2004). Crisis: A Watershed From Local, Specific Turbulences, to Global, Inconceivable Crises in Unstable and Torn Environments, Future Crises. In the International Workshop, Future Agendas: An Assessment of International Crisis Research,

Lagadec, P. and Michel-Kerjan, E. (2004) "Meeting the Challenge of Interdependent Critical Networks under threat: The Paris Initiative, Anthrax and Beyond," Cahier No. 2004-014, Laboratoire D'Econometrie, Ecole Polutechnique, Paris.

Lewis, P.R. and Reynolds, K. (2002). Forensic Engineering: A Reappraisal of the Tay Bridge Disaster. Interdisciplinary Science Reviews, 27(4), pp. 287-298.

Luhmann, N. (1990). Technology, environment and social risk: a systems perspective. Industrial Crisis Quarterly, Vol. 4, No. 3, pp. 223-231.

Mahon, J.F. and Cochran, P.L. (1991). Fire Alarms and Siren Songs: the role of issues management in the prevention of, and response to, organisational crises. Industrial Crisis Quarterly, 5, pp. 155-176.

Marais, K., Dulac, N. and Leveson, N. (2004). Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems. Presented at the Engineering Systems Division Symposium, MIT, Cambridge, MA, March 29-31.

Mason, R.O. (2004). Lessons in Organisational Ethics from the Columbia Disaster: Can a culture be lethal? Organisational Dynamics, 33 (2), pp.128-142.

Mendonça, S. Pina e Cunha, M., Kaivo-oja, J. and Ruff, F. (2004). Wild cards, weak signals and organisational improvisation. Futures, 36(2), pp.201-218.

Mileham, G. (1998) *The Tay Railway Bridge* http://web.archive.org/web/20020609121056/http://www.brad.ac.uk/acad/civeng/marketing/civeng/failtay1.htm accessed 17/02/2005 2:04 PM,

Mitroff, I.I., and Alpaslan, M.C. (2003) "Preparing for Evil," In: the *Harvard Business Review*, April, 109-115.

Mitroff, I.I., and Kilmann, R.H. (1984). Corporate Tragedies: Product Tampering, Sabotage, and other Catastrophes, Praeger, New York.

November 24-26, Sophia-Antipolis (Nice), France.

Nystrom, P.C. and Starbuck, W.H. (1984). To Avoid Organisational Crises, Unlearn. Organisational Dynamics, 12(4), pp. 53-65.

OECD (2003). Security in Maritime Transport: Risk factors and Economic Impact, Maritime Transport Committee, Directorate for Science, Technology and Industry, July.

Pearson, C.M. and Clair, J.A. (1998). Reframing Crisis Management. Academy of Management Review, 23(1).

Pearson, C.M. and Mitroff, I.I. (1993) "From Crisis prone to Crisis Prepared: A framework for crisis management," In: *Academy of Management Executive*, 7(1), pp. 48-59.

Perrow, C. (1984). Normal Accidents: Living with High Risk Technologies, Basic Books, New York.

Pinsdorf, M.K. (1997). Engineering into Disaster: History of the Tay Bridge. Business and Economic History, 26 (2), pp. 491-504.

pp. 4–10

Revans, R, (1982). The Origins and Growth of Action Learning, Chartwell-Bratt, Bromely.

Boin, R., Rhinard, M. and Ekengren M., (2004) Functional Security and Crisis Management Capacities in the European Union: Setting the Research Agenda. *Research Proposal*, CRC/ Eurosec, 30 May.

Rijpma, J.A. (1997). Complexity, Tight-coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory. Journal of Contingencies and Crisis Management, (5)1: pp. 15-23.

Ringland, G. *et.al.* (1999). Shocks and Paradigm Busters (Why do we get surprised). Long Range Planning, 32 (4), pp. 403-413.

Roberts, K.H. Rousseau, D.M. and La porte, T.R. (1994). The Culture of High Reliability: Quantitative and qualitative assessment aboard nuclear-powered aircraft carriers. Journal of High Technology Management Research, 5(1), pp. 141-161.

Roberts, K.H. (1990a). Managing Reliability Organisations.California Management Review, 32(4), pp. 101-114.

Roberts, K.H. (1990b). Some Characteristics of one type of High Reliability Organisation. Organisational Science, 1(2), pp. 160-176.

Robertson, D.A. (2004).The Complexity of the Corporation. Human Systems Management (23), pp. 71-78.

Sarewitz, D. and Pielke Jr., R. (2001).Extreme Events: A Research and Policy Framework for Disasters in Context. International Geology Review, 43(5), pp. 406-418. .

Shannon, C.E. (1949). The Mathematical Theory of Communications, University of Illinois Press, Urbana.

Smart C. and Vertinsky, I. (1977). Designs for Crisis Decision Units. Administrative Science Quarterly, Vol. 22, pp640-657

Stead, E. and Smallman, C. (1999). Understanding Business failure: Learning and Un-learning Lessons from Industrial Crises. Journal of Contingencies and Crisis Management, 7(1), pp. 1-18.

Tompkins, P.K (1993). Organisational Communication Imperatives: Lessons of the Space Programme, Trans-Atlantic Pubs.

Turnbull S. (2002). The Science of Corporate Governance. Corporate Governance, October, 10(4), pp. 261-277.

Turner, B.A. (1994). Causes of Disaster: Sloppy Management. British Journal of Management, 5, pp.215-219.

Turner, B.A. and Pidgeon, N. (1997). Man-made Disasters (2nd edn), Butter-worth Heineman, Oxford.

Weick, K. E. (1988). Enacted Sense Making in Crisis Situations. Journal of Management Studies, 24(4).
Weick, K.E. (2004). Normal Accident Theory as Frame, Link and Provocation. Organization & Environment, 17(1), pp. 27-31.
Weir, D. (2004). Sequences of Failure in Complex Socio-technical Systems: Some implications of decision and control. Kybernetes, 33(3/4), pp. 522-537.
Wisenblit, J. Z. (1989). Crisis Management Planning Among U.S. Corporations: Empirical Evidence and a Proposed Framework. S.A.M. Advanced Management Journal 54(2), pp. 31-41.